REMARKS

Claim 41 had been presented twice in the previous response. Accordingly, the second presentation of claim 41 had been considered (but not officially denoted as) claim 42 in the last response. To avoid confusion, the claims numbered 41 are cancelled and replaced with identically-written claims 42 and 43.

Applicants respectfully traverse the indefiniteness rejection of claim 40. Consider the usual flowchart -- it will have often have decision blocks containing a question having a yes or no answer. If you answer yes, you go down one branch in the flowchart whereas if you answer no you go down another branch. This type of conditional branching is quite definite and very commonly used in claims. Indeed, Applicants note that Richard reference (USP 5,922,074) cited in the 11/3/04 office action is absolutely _rife_ with the use of "if" statements in its claims. For example, consider claim 1 of this patent, which recites the step of "verifying that said digital certificate is valid." Clearly, there are two results obtainable in response to such a step: either the certificate is verified as valid or it is not. Thus, the claim then recites the step of "retrieving, _if_ the digital certificate is valid, an access control rule..." This conditional statement is not indefinite at all: it follows definitely from the previous act.

More fundamentally, Applicants note that the statutes, caselaw, and MPEP § 2173 set forth absolutely no such rule (that "if" renders claims indefinite). Here, claim 40 limits claim 36. Claim 36 is directed to a method of revoking a host device. This revocation is responsive to the act of "applying the at least one rule on the data in the revocation file and the associated data in the certificate." There can only be two outcomes with respect to revocation: the host is revoked or the host is not revoked. Thus,

<div align="center">Page 5 of 10</div>

Appl. No.: 09/939,896

claim 40 sets forth the act of "if the application of the at least one rule provides a successful result, granting the file request." In other words, that host is not revoked should the application of the at least one rule provide a successful result. There is no indefiniteness to such conditional language -- it is just as definite as that used in claim 1 of USP 5,922,074. Accordingly, because this conditional language is definite and because the use of conditional language is not proscribed by the statutes, caselaw, or by the MPEP, Applicants respectfully request that the indefiniteness rejection be withdrawn. The indefiniteness objection to what is now claim 43 is traversed on the same grounds.

Applicants respectfully traverse the obviousness rejections of the pending claims.

Authentication methods in digital rights management (DRM) schemes are known. Indeed, both the Graunke reference (USP 5,991,399) and the Richard reference (USP 5,992,074) recognize their use. Content providers provide digital certificates to content users so that they become authorized to access protected content. For example, a user at a host device such as a personal computer may obtain a digital certificate that is then provided to a storage engine controlling access to protected content stored on a storage medium. The authentication process comprises verifying a digital signature provided by the content provider that is contained within the digital certificate. Once the signature is authorized, the user is authenticated and may proceed to access the protected content.

However, because digital signatures involve the use, typically, of private/public key cryptography that may become compromised, there is another layer of protection commonly available in conventional DRM schemes. That layer would be the revocation process, which follows authentication. In other words, even though a user may possess a

valid certificate, if that user is identified by a revocation list, the user is denied access to the protected content.

As is conventional, this revocation scheme follows authentication. It is performed as an initial handshaking routine between the host device and the storage engine.

In contrast to the conventional revocation scheme just discussed, the present invention provides a file-by-file revocation scheme. It is not performed immediately following authentication but instead is much more granular in that it precedes any file request by the host device. Consider, for example, pages 32 and 33 of the disclosure. As set forth by the Applicants, in their revocation scheme, each file may have its own associated revocation list, see for example, lines 21 through 23 on page 32. As such, this type of revocation would not be performed immediately after authentication – a user may or may not desire access to any given file on the storage medium. Not only do the Applicants provide greater granularity and control, the revocation itself is more adaptable in that the associated revocation list with a given file comprises a set of rules for evaluating fields in the digital certificate against data in the revocation list, see for example lines 24 through 28 on page 32.

These advantageous features of Applicants revocation scheme are reflected in the claims. For example, claim 36 recites a revocation method including the acts of: authenticating the digital signature; receiving at the storage engine a file request from the host device, the file request being directed to a file stored on a storage medium accessible to the storage engine; reading a revocation file associated with the file from the storage medium, the revocation file containing at least one rule, the at least one rule associating data in the revocation file with data in certificate; applying the at least one rule on the

data in the revocation file and the associated data in the certificate; and if the application of the at least one rule provides a failing result, denying the file request.

In sharp contrast, consider the Graunke reference, which is merely directed to a key distribution scheme. As seen in Figure 2, a "trusted player" provides a "signed manifest" to the server, which then distributes a key using key generation module (element 50). Note that the claim is instead directed to a storage engine revoking a host, not a storage engine requesting a key. There is absolutely no suggestion in Graunke for the acts of "receiving at a storage engine a certificate from the host device, the certificate containing a digital signature (in Graunke, the storage engine provides the "signed manifest"); ....; reading a revocation file associated with the file from the storage medium, the revocation file containing at least one rule, the at least one rule associating data in the revocation file with data in certificate; applying the at least one rule on the data in the revocation file and the associated data in the certificate; and if the application of the at least one rule provides a failing result, denying the file request (in Graunke, the storage engine is merely obtaining a decryption key from the server).

The Richard reference adds nothing further. Richard merely discloses a "distributed" identification scheme that does not require a meta-certifier, "who must certify all users in order to provide the desired level of security." Col. 2, lines 8-9. In this distributed scheme, a clients seek content from servers across a distributed network as seen in Figure 1. As part of this process, the client provides a digital certificate as seen in Figure 3. Once the client is established as a trusted device, the authentication process is done: just like the conventional authentication schemes discussed by the Applicants. There is absolutely no suggestion for a file-by-file granular revocation scheme as claimed

by the Applicants. In that regard, the identification and verification process performed

between the server and client with respect to the digital certificate provided by the client

is shown in Figure 6a and 6b. In particular, note step 92 in Figure 6a which asks whether

the certificate is valid. If so, then in step 94 the "directory cross references the client

certificate, the server certificate, and the communications context to retrieve an internally

stored Access Control Rule to apply to the client connection." Figure 7 simply shows an

"exemplary verification descriptor object/data structure" with respect to Figures 6a and

6b.

Once the Richard process is complete, the authentication and identification

process is done – there is absolutely no teaching or suggestion for the granular file-by-file

revocation process as claimed. Moreover, and even more fundamentally, there is

absolutely no suggestion for a revocation scheme at all with respect to a storage engine

receiving file requests from a host.

Applicants urge that the digital rights management (DRM) field is a crowded art,

using well-known techniques and principles. Developments in DRM build upon these

known principles and techniques. It is entirely improper to use hindsight in judging

whether a DRM development is non-obviousness: indeed, DRM developments in general

will typically appear obvious in HINDSIGHT. But that is not how an obviousness

analysis is conducted. The present claims are plainly patentable over the art of record.

With the prior art of record, one can only say "well, they don't teach or suggest your

invention but I still think it would be obvious to provide such a granular revocation

scheme." That obviousness conclusion can only be grounded in hindsight based upon the

prior art of record.

Because claims 37 through 40 depend either directly or indirectly upon claim 36, they are patentable for at least the same reasons.

Claims 42 and 43 are apparatus claims that are patentable analogously as discussed with respect to claim 36.

Claim 40 has been amended to address a minor typographical error.

CONCLUSION

For the above reasons, pending Claims 36-40, 42, and 43 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

Certification of Facsimile Transmission
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.
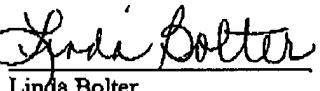
Linda Bolter   __November 16, 2004__

Linda Bolter   Date of Signature

Respectfully submitted,
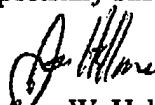
Jonathan W. Hallman
Attorney for Applicants
Reg. No. 42,622